REMARKS

The August 12, 2008 Office Action was based upon pending Claims 1, 5, 7, 8, 12-14, 17 and 20-24. This Amendment amends Claims 1, 5, 7, 8, 13, 17, 22, and 24. Thus, after entry of this Amendment, Claims 1, 5, 7, 8, 12-14, 17 and 20-24 are pending and presented for further consideration.

ISSUES RAISED IN THE OFFICE ACTION

The Office Action objected to Claims 1, 8 and 22 for a variety of informalities.

The Office Action also objected to the introduction of new matter associated with previous amendments made to Claims 1, 5 and 8.

The Office Action rejected Claims 1 and 5 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

Further, the Office Action rejected Claims 1, 5, 8, 12, 13, 17, 20-22 and 24 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,178,021 to Hanna, et al. (hereinafter "Hanna"), in view of U.S. Patent No. 4,864,616 to Pond, et al. (hereinafter "Pond"), in view of U.S. Publication No. 2001/0039659 to Simmons, et al. (hereinafter "Simmons"), and further in view of U.S. Patent No. 6,310,692 to Fan, et al. (hereinafter "Fan").

In addition, the Office Action rejected Claims 7, 14 and 23 under 35 U.S.C. §103(a) as being unpatentable over Hanna, in view of Pond, in view of Simmons, in view of Fan, and further in view of U.S. Patent No. 6,094,721 to Eldridge, et al. (hereinafter "Eldridge").

OBJECTION OF CLAIMS 1, 8 AND 22

The Office Action objected to Claims 1, 8 and 22 for a variety of informalities.

Claim 1

The Office Action states that the use "client computer system" in Claim 1 should be "first computer system." In response, Applicant has made this change to Claim 1.

Claim 8

The Office Action states that the use of "client computer system" in Claim 8 should be "first computer system." In response, Applicant has made this change to Claim 8.

Claim 22

The Office Action states that the use of "client computer system" in Claim 22 should be "first computer system." In response, Applicant has made this change to Claim 22.

OBJECTION OF PREVIOUS AMENDMENTS MADE TO CLAIMS 1, 5 AND 8.

The Office Action also objected to the introduction of new matter associated with previous amendments made to Claims 1, 5 and 8. While Applicant does not believe that the proposed amendments introduce new matter, Applicant has removed the objectionable language.

REJECTION OF CLAIMS 1 AND 5 UNDER 35 U.S.C. §112

The Office Action rejected Claims 1 and 5 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

Claim 1

With respect to Claim 1, the Office Action rejected the phrase "the client computer system uniquely retains a private key" and "wherein both the encryption key and the private key are needed for decryption of encrypted data.

In response, Applicant has deleted this language.

Claim 5

With respect to Claim 5, the Office Action rejected "wherein both the public and the private encryption keys are needed to decrypt encrypted data." In response, Applicant has deleted this language.

REJECTION OF CLAIMS 1, 5, 8, 12-13, 17, 20-22 AND 24 UNDER 35 U.S.C. §103(a)

The Office Action rejected Claims 1, 5, 8, 12, 13, 17, 20-22 and 24 under 35 U.S.C. §103(a) as being unpatentable over Hanna, in view of Pond, in view of Simmons, and further in view of Fan.

Claim 1

Claim 1 is directed to a method of transferring data over a computer network from a network server to a first client computer system, the method comprising receiving a request by a requestor using a first client computer system for data from at least one network server storing data, at least some of the data stored by the network server being encrypted.

New Encryption Key When Verification Fails

The method of Claim 1 verifies whether a public encryption key associated with the requestor is good and if verification fails, requesting user input from the requestor and generating a public encryption key and a private encryption key.

The generated public and private encryption keys are based at least in part on the user input and based at least in part on an identification code associated with the first client computer system.

None of the cited references teach or suggest the verification of the public encryption key associated with the requestor. Furthermore, none of the cited references describe generating new public and private keys based on 1) user input and 2) an identification code associated with the first client computer system.

Therefore, Applicant respectfully asserts that Claim 1 is not obvious in view of the cited references.

The Unique Attribute Stored On The Network Server

Furthermore, when a requestor requests data stored on the network server, the method checks an attribute of the requested data to determine whether the requested data stored on the network server is encrypted with an the public encryption key associated with the requestor.

If the attribute stored on the network server indicates that the requested data stored on the network server is encrypted with the public encryption key associated with the requestor, the method automatically sends the encrypted data to the first client computer system.

If the attribute stored on the network server indicates that requested data is encrypted with a public encryption key that is different than the public encryption key associated with the requestor, the method automatically sends a message to the requestor indicating that the requested data is not encrypted with the public encryption key of the requestor.

If the attribute stored on the network server indicates that the requested data is unencrypted, automatically retrieving the encryption key associated with the requestor from the first client computer system and encrypting the requested data stored on the server with the public encryption key associated with the requestor automatically and without user intervention to create encrypted data.

None of the cited references teach or suggest such a unique attribute stored on the network server that indicates 1) whether the data is encrypted with the requestor's public encryption key, 2) whether the requested data is encrypted with a different public encryption key and 3) whether the requested data is unencrypted.

While the Office Action attempts to combine various references to address these instances, none of the cited references have an attribute that provides these indications. Accordingly, Applicant respectfully asserts that Claim 1 is not obvious in view of the cited references.

Automatic Action Based On The Unique Attribute

Still further, none of the cited references describe automatically taking different actions based on the unique attribute. For example, the method automatically sends the encrypted data if the data is encrypted with the requestor's public key.

Likewise, the method automatically sends a message to the requestor if the data is encrypted with a different public key.

In addition, the method automatically encrypts the data with the requestor's public key if the data is not encrypted.

Because none of the cited references describe automatically taking such actions, Applicant respectfully asserts that Claim 1 is not obvious in view of the cited references.

Improper Finding of Obviousness

Section 2143 of the M.P.E.P. states that to establish prima facie obviousness three requirements must be met:

> "To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure."

In the present case, none of the three requirements have been met. In particular, even when the cited references are combined, they do not teach the elements of Claim 1. Applicant therefore respectfully submits that Claim 1 is patentably distinguished over the cited references and Applicant respectfully requests allowance of Claim 1.

Furthermore, the case, *KSR International Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 82 U.S.P.Q.2d 1385 (2007), in no way relieves the Patent Office of its obligation to "consider ***all claim limitations*** when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (emphasis added). Accordingly, it remains well settled law that a finding of "obviousness requires a suggestion of ***all limitations*** in a claim." *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (emphasis added) (cited in *Ex Parte Wada*, 2008 WL 142652, *4 (Bd.Pat.App. & Interf., Jan. 14, 2008)).

In the aftermath of KSR, the Board of Patent Appeals and Interferences has repeatedly reversed findings of obviousness when the Examiner has failed to proffer a

prima facie case of obviousness. See, e.g., *Wada*, 2008 WL 142652 at *5 ("Because the Examiner has not explained why ***every limitation*** in claim 1 would have been obvious to a person of ordinary skill in the art, we agree with Appellants that the Examiner has not made out a case of prima facie obviousness.") (emphasis added); *Ex Parte Challapali*, 2008 WL 111346, *4-6 (Bd.Pat.App. & Interf., Jan. 10, 2008) (reversing finding of obviousness because the Examiner failed to establish sufficient reasoning for combining the references).

The Examiner Has Not Presented a Prima Facie Case of Obviousness

In view of the arguments set forth herein, Appellant submits that Claim 1 is patentable over the cited references based on at least the following elements:

1) verifying the requestor's encryption key,

2) if verification fails, generating public and private encryption keys based on user input and based on an identification code associated with the first client computer system,

3) a unique attribute stored on the network server that indicates a) whether the data is encrypted with the requestor's public encryption key, b) whether the requested data is encrypted with a different public encryption key and c) whether the requested data is unencrypted, and

4) automatically taking different actions based on the unique attribute.

Thus, in order to establish a prima facie case of obviousness for the pending claims, the Examiner must present, inter alia, references that when combined have each and every claim limitation. However, neither of the combined references suggests such limitations. Thus, Appellant respectfully contends that the Examiner has failed to provide adequate articulation of his reasoning to support the legal conclusion of obviousness.

Dependent Claims 12 and 13

Claims 12 and 13 depend from Claim 1 and are believed to be patentable for the same reasons articulated above with respect to Claim 1, and because of the additional features recited therein.

Claim 5

Claim 5 is directed to a method of data storage and retrieval comprising verifying whether a public encryption key associated with a requestor is good and if verification fails, requesting user input and automatically generating independently of information from a network server, a public encryption key and a corresponding private encryption key in a first client computer system based at least in part on the user input and based at least in part on an identification code associated with the first client computer system, wherein the network server stores at least some data in an encrypted format.

The method further comprises storing the public encryption key and the corresponding private encryption key in the first client computer system such that access to the private encryption key is limited solely to the first client computer system and wherein both the public and the private encryption keys are needed to decrypt encrypted data.

The method also comprises associating an attribute with a data file on the network server, the attribute indicating whether the data file is encrypted with the public encryption key associated with different requestors when stored on the network server, and the attribute indicating an owner of the public encryption key.

In addition, the method comprises requesting the data file by a requestor from the network server using the first client computer system and checking the attribute of the requested data file to determine whether the requested data file is encrypted with the public key of the requestor.

Furthermore, if the attribute stored on the network server, the method indicates that the requested data is encrypted with a public encryption key that is not associated with the requestor, sending a message to the requestor indicating that the requested data is not encrypted with their key.

Also, if the attribute stored on the network server indicates that the requested data file is encrypted with the public key associated with the requestor, the method forwards the requested data file to the first client computer system.

In addition, if the attribute stored on the network server indicates that the requested data file is unencrypted, the method sends the public encryption key from the first client computer system to the network server automatically and without user intervention.

Further, the methods forwards the requested data file to the first client computer system after the public encryption key associated with the requestor is used to encrypt the requested data file to create an encrypted data file wherein the encrypted data file is forwarded to the requestor.

The method also automatically decrypts, without user intervention, the encrypted data file with the private encryption key in the first client computer system.

Because none of the cited references describe these unique concepts, Applicant respectfully asserts that Claim 5 is not obvious in view of the cited references. In addition, although Claim 5 has different language than Claim 1, Claim 5 is believed to be patentable for similar reasons (where applicable), and because of the different features recited therein.

Accordingly, Applicant respectfully asserts that Claim 5 is not obvious in view of the cited references and Applicant respectfully requests allowance of Claim 5.

Dependent Claim 17

Claim 17 depends from Claim 5 and is believed to be patentable for the same reasons articulated above with respect to Claim 5, and because of the additional features recited therein.

Claim 8

Claim 8 is directed to a computer readable data storage medium having stored thereon commands that are operative to cause a general purpose computer configured as a network server to perform a method of data retrieval comprising verifying whether an encryption key associated with a requestor is good and if verification fails, requesting user input from the requestor and generating an encryption key based at least in part on the user input and based at least in part on an identification code associated with the first client computer system.

Claim 8 also comprises receiving a request for a data file from a requestor using a first client computer system at a network server, wherein at least some data files are encrypted and checking a file attribute of the requested data file stored on the network server to determine whether the requested data file is encrypted with the encryption key associated with the requestor, wherein the attribute is alterable by a network administrator.

In addition, if the file attribute stored on the network server indicates that the requested data file is encrypted with the encryption key associated with the requestor, routing the encrypted data file to the first client computer system. Also, if the file attribute stored on the network server indicates that the requested data file is encrypted with an encryption key that is different than the encryption key associated with the requestor, sending a message to the requestor indicating that the requested data is not encrypted with the encryption key associated with the requestor.

Furthermore, if the file attribute stored on the network server indicates that the requested data file is unencrypted, automatically requesting the public encryption key associated with the requestor from the first client computer system.

Claim 8 also comprises automatically encrypting the requested data file using the public encryption key associated with the requestor to create an encrypted data file; routing the encrypted data file to the first client computer system; and automatically decrypting without user intervention the encrypted data file with the private encryption key associated with the requestor.

Because none of the cited references describe these unique concepts, Applicant respectfully asserts that Claim 8 is not obvious in view of the cited references. In addition, although Claim 8 has different language than Claim 1, Claim 8 is believed to be patentable for similar reasons (where applicable), and because of the different features recited therein.

Accordingly, Applicant respectfully asserts that Claim 8 is not obvious in view of the cited references and Applicant respectfully requests allowance of Claim 8.

Dependent Claims 20-22 and 24

Claims 20-22 and 24 depend from Claim 8 and are believed to be patentable for the same reasons articulated above with respect to Claim 8, and because of the additional features recited therein.

REJECTION OF CLAIMS 7, 14 AND 23 UNDER 35 U.S.C. §103(a)

In addition, the Office Action rejected Claims 7, 14 and 23 under 35 U.S.C. §103(a) as being unpatentable over Hanna, in view of Pond, in view of Simmons, in view of Fan, and further in view of Eldridge.

Claim 7

Claim 7 depends from Claim 5 and is believed to be patentable for the same reasons articulated above with respect to Claim 7, and because of the additional features recited therein.

Claim 14

Claim 14 depends from Claim 1 and is believed to be patentable for the same reasons articulated above with respect to Claim 1, and because of the additional features recited therein.

Claim 23

Claim 23 depends from Claim 8 and is believed to be patentable for the same reasons articulated above with respect to Claim 8, and because of the additional features recited therein.

NO DISCLAIMERS OR DISAVOWALS

Although the present communication may include alterations to the application or claims, or characterizations of claim scope or referenced art, Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application.

Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution.

Accordingly, reviewers of this or any parent, child or related prosecution history shall not reasonably infer that Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

CO-PENDING APPLICATIONS OF ASSIGNEE

Applicant wishes to draw the Examiner's attention to the following co-pending applications of the present application's assignee.

Serial Number	Filed	Status	Attorney No.	Title
11/452,594	06/14/2006	Pending Office Action	MTIPAT.187C1	Data Security For Digital Data Storage
11/521,163	09/14/2006	Pending Office Action	MTIPAT.187DV1	Data Security For Digital Data Storage
09/277,482	03/26/1999	Issued – Pat. No. 6,857,076	MTIPAT.075A	Data Security For Digital Data Storage
10/962,997	10/12/2004	Issued – Pat. No. 7,114,082	MTIPAT.075C1	Data Security For Digital Data Storage
11/524,097	09/20/2006	Pending	MTIPAT.075C2	Data Security For Digital Data Storage
09/277,335	03/26/1999	Issued – Pat. No. 7,096,370	MTIPAT.076A	Data Security For Digital Data Storage
11/503,101	08/11/2006	Pending	MTIPAT.076C1	Data Security For Digital Data Storage

Applicant notes that cited references, office actions, responses and notices of allowance have occurred or will occur for the above-referenced matters. In particular, Applicant notes that Office Actions were recently received for U.S. Patent Application Nos. 11/452,594 and 11/521,163.

Applicant also understands that the Examiner has access to sophisticated online Patent Office computing systems that provide ready access to, for example, specification and drawing publications, pending claims and complete file histories, including, for example, cited art, office actions, responses, and notices of allowance.

Applicant respectfully requests that the Examiner continue to review these file histories for current information about these matters. Also, if the Examiner cannot readily access these file histories, the Applicant would be pleased to provide any portion of any of the file histories at any time upon specific Examiner request.

CONCLUSION

Applicant has endeavored to address all of the Examiner's concerns as expressed in the outstanding Office Action. In light of the above remarks, reconsideration and withdrawal of the outstanding rejections is specifically requested.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 11-12-08

By: John R. King

John R. King
Registration No. 34,362
Attorney of Record
Customer No. 20,995
(949) 760-0404

6226569
111208